IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

In re: Equifax, Inc. Customer Data Security Breach Litigation	)	MDL Docket No. 2800
	)	Case No.: 1:17-md-2800-TWT
	)	
	)	**CONSUMER TRACK**
	)	**SMALL BUSINESS COMPLAINT**
	)	

SMALL BUSINESS PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO EQUIFAX'S MOTION TO DISMISS THE SMALL BUSINESS COMPLAINT

TABLE OF CONTENTS

TABLE OF CASES

INTRODUCTION

The main consolidated consumer complaint before this Court (Doc. 374) was filed on behalf of the nearly 150 million individual victims of the Equifax data breach. That complaint seeks damages sustained by individual consumers, including recovery of out-of-pocket losses and reimbursement of the cost of buying products to mitigate the risk of fraud. At issue here is the complaint filed by Small Business Plaintiffs, such as Subchapter S corporations and limited liability companies, which are separate and distinct legal entities. The Small Business Plaintiffs, which rely on the personal creditworthiness of individual consumers to obtain and maintain credit, seek to recover their own out-of-pocket losses and mitigation costs resulting from the breach, damages that belong only to them and are not recoverable by the individual consumer plaintiffs.

Equifax erroneously argues that the small business complaint should be dismissed for reasons similar to those asserted in its motion to dismiss the consumer complaint with one major difference: according to Equifax, the Small Business Plaintiffs did not themselves lose personal information in the breach, and thus, as a matter of law, any harm to them is too remote and attenuated to support civil liability. The Small Business Plaintiffs acknowledge that they must establish an extra step in the causal chain, but they are no less foreseeable victims than their

consumer owners, have their own injuries directly attributable to the breach and, as a result, have viable legal claims. The Court should reject each of Equifax's three primary arguments to the contrary.

First, Equifax contests the Article III standing of the Small Business Plaintiffs, unlike that of the consumer plaintiffs. Ample precedent establishes that the Small Business Plaintiffs allege concrete injuries fairly traceable to Equifax's conduct, however, which is all that is required at the pleading stage. Small businesses were forced to purchase credit reports and monitoring to protect against the substantially certain risk of harm from the breach—the same exact type of foreseeable harm that Equifax has long urged small businesses to protect themselves against by buying *Equifax* products. Indeed, after the breach, numerous Congressional committees and commentators recommended that small businesses take these specific measures. Accordingly, the costs to small businesses are not, as Equifax urges, the result of an attenuated chain of events, but rather the type of concrete harm Equifax knew would result from a breach of this magnitude.

Second, Equifax owed a tort duty not to subject small businesses to an unreasonable risk of harm. While differently situated from the consumer plaintiffs, the Small Business Plaintiffs are comfortably within the zone of foreseeable harm from a breach, triggering Equifax's duty to exercise reasonable care for their

protection. Consequently, for the same reasons as argued by the consumer plaintiffs, this Court's rulings in *Home Depot* and *Arby's* control and the *McConnell* decisions relied on by Equifax are inapposite.

Third, these claims do not fail under the doctrine of proximate cause, nor are they barred by the economic loss rule. Equifax's authorities are distinguishable because they involve business interruptions so remote that Georgia courts have—following hornbook law—determined that liability cannot attach. Where, as here, the facts show that Equifax knew the risk of this specific harm to this specific type of victim, the intertwined fact questions of foreseeability, proximate cause, and the economic loss bar cannot be determined on a Rule 12 motion. The small business claims thus are factually plausible and legally sufficient.

FACTUAL BACKGROUND

The Small Business Complaint (Doc. 375) describes Equifax's business model, special role in the modern economy as a compiler and steward of confidential information, long history of data security failings and knowledge that a massive breach was likely to occur, willful failure to protect consumer personal information that small businesses rely on for credit and continued operation, and untimely and insufficient response to the breach. Compl. ¶¶ 30-189.

While those allegations mirror the allegations of the main consumer complaint, the Small Business Complaint avers that individual consumers are not the only victims of the breach. Small businesses obtain and maintain financing based, in large part, on their owners' personal financial situation. Identity theft, fraud, and other adverse events affecting a small business owners' personal creditworthiness—which has occurred as a result of the Equifax data breach—directly and immediately impact the business by reducing its access to credit, increasing its borrowing costs, reducing the value of its collateral, and ultimately jeopardizing its operations. Compl. ¶¶ 190-94. As a result, the theft of confidential financial information belonging to a consumer victimized by the Equifax data breach also threatens the financial affairs of any small business owned by that consumer. Similarly, the resulting substantially certain risk of imminent harm justifies a small business to take measures to mitigate the separate risk that it faces. *Id.*

In the wake of the Equifax breach, Congressional committees recognized "the significant potential exposure to small businesses as a result of the breach" because the "availability of business credit for small business owners is inextricably tied to their personal credit score"; stated that they were "gravely concerned about the effect this breach will have on the ability of small businesses

to access affordable credit"; and warned that the breach "could be devastating for these businesses and their ability to get credit on reasonable terms." *Id.* ¶¶ 195-96. Accordingly, the committees told Equifax it "has an obligation to make this right" by providing means for small businesses to protect themselves. *Id.* ¶ 197. Likewise, trade publications warned small businesses that the breach posed an imminent threat to their credit and viability, *id.* ¶¶ 198-99, and touted credit monitoring services sold specifically to businesses (as differentiated from those sold to individual consumers) as essential protection against the threat, *id.* ¶¶ 200, 206. Following these warnings, many small businesses purchased credit report and monitoring products for their business, including those named as plaintiffs in this action.

The risk to a small business posed by a data breach involving its owner's confidential information is both real and foreseeable. This risk is evidenced by the fact that commercial products are available to enable small businesses to detect and mitigate the risk. Indeed, Equifax itself sells such products. *Id.* ¶¶ 201-05. Perhaps most cynically, *after the breach*, Equifax introduced and continues to sell a product to small businesses designed to mitigate the very harm Equifax created (and then discounts by its Motion), rejecting an explicit request by Congressional committees that such "protective products" be provided free of charge. *Id.* ¶¶ 6, 207-09, 211. In

light of the sale of these products, there can be no question that Equifax knew small businesses would be harmed by a data breach and would need to buy credit reports and credit monitoring services to detect and mitigate that harm. *Id.* ¶ 210.

In short, Small Business Plaintiffs were damaged by the Equifax data breach and remain subject to a pervasive, substantial, and imminent risk of fraud and negative credit consequences flowing from the unauthorized dissemination of their owners' personal information. *See, e.g.*, *id.* ¶¶ 5, 11-21, 190-211. Accordingly, notwithstanding that their losses are in one sense derivative of those suffered by consumer plaintiffs, the Small Business Plaintiffs have valid and distinct legal claims separate and apart from their owners that should not be dismissed.

LEGAL STANDARD & CHOICE OF LAW

A complaint may only be dismissed if the facts alleged fail to state a "plausible" claim. *In re: The Home Depot, Inc. Customer Data Security Breach Litig.*, 2016 WL 2897520, at *3 (N.D. Ga. May 18, 2018) (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 677 (2009); Fed. R. Civ. P. 12(b)(6)). A claim survives even if it is "improbable" a plaintiff will be able to prove those facts or the odds of recovery are "remote and unlikely." *Id.* (citing *Bell Atlantic v. Twombly*, 550 U.S. 544, 556 (2007)). "[T]he court must accept the facts pleaded in the complaint as true and construe them in the light most favorable to the plaintiff." *Id.*

Equifax asserts that Georgia law applies to the common law claims for purposes of this motion. Mot. 10 & n.2. Plaintiffs agree that the Court need not apply the common law of other states, unless it decides that Georgia law is adverse to the common law claims of the national class pled in the Complaint, in which case it will be necessary to consider the common law of each state applicable to the proposed alternative, state-specific classes. *See* Compl. ¶ 213 (pleading alternative claims based on the common law of each plaintiff's home state).

ARGUMENT

I. SMALL BUSINESS PLAINTIFFS HAVE ARTICLE III STANDING.

In determining Article III standing, the Court must evaluate whether the Small Business Plaintiffs properly pleaded that they "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendants, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). Equifax did not challenge the Article III standing of the consumer plaintiffs, but contends that the Small Business Plaintiffs' Complaint is "devoid of plausible factual allegations" necessary to support the "injury" and "traceability" elements of Article III standing. To reach this conclusion, Equifax mischaracterizes and ignores Plaintiffs' well-pled allegations. When considering

the allegations actually set forth in the Complaint, this Court should readily conclude that Plaintiffs have Article III standing to pursue their claims.

A. The Complaint Details That Plaintiffs Have Been Injured.

Plaintiffs detail how the vast majority of small businesses depend on their owners' personal credit in order to fund their operation, meaning that the owners' personal creditworthiness is critical for small businesses to survive. Compl. ¶¶ 190-94. Further, as noted above, numerous governmental entities and independent reporters have recognized that where the personal information of a small business owner is compromised, the owner's business is also at risk, may suffer adverse financial consequences, and must take protective measures. *Id.* ¶¶ 195, 197, 206. Because their owners' personal information was compromised in the Equifax breach, Small Business Plaintiffs allege that they incurred direct, out-of-pocket costs in responding to, and mitigating the impact of, the breach, such as purchasing business credit reports (including those marketed and sold by Equifax) and devoting resources to monitoring financial accounts. Compl. ¶¶ 11-21, 202-206. Plaintiffs' allegations are sufficient to satisfy the requirements of Article III at the pleading stage, as explained below.

B. The Complaint Alleges A Cognizable Injury-In-Fact.

To establish injury-in-fact, a plaintiff must show that he or she suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (quotations omitted). As the Supreme Court has recognized, "[a]t the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we 'presum[e] that general allegations embrace those specific facts that are necessary to support the claim.'" *Id.* at 561; *see also Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1323 (11th Cir. 2012). Further, to properly plead an injury-in-fact, the Supreme Court has held that plaintiffs need not "demonstrate that it is *literally certain* that the harms they identify will come about. In some instances, we have found standing based on a '*substantial risk*' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013) (emphases added).[1]

[1] Citing *Clapper*, Equifax asserts that "[t]he Business Plaintiffs 'cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm.'" Mot. 16. But *Clapper* was referring to a highly speculative situation where plaintiffs challenged a provision of the Foreign Intelligence Surveillance Act that allowed surveillance of foreign nationals outside the United States; the plaintiffs were not foreign nationals themselves, they alleged only an "objectively reasonable likelihood" that their communications with

This Court has held in two cases that allegations of mitigation costs incurred reducing the substantial risk of harm from a data breach, such as those made here by the Small Business Plaintiffs, are sufficient to confer Article III standing under *Clapper*. *See Home Depot*, 2016 WL 2897520, at *3 (holding that "any costs undertaken to avoid future harm from the data breach would fall under footnote 5 of *Clapper*, specifically as reasonable mitigation costs due to a substantial risk of harm."); *In re Arby's Rest. Grp. Inc. Litig*., 2018 WL 2128441, at *11 (N.D. Ga. March 5, 2018) (holding that allegations related to "costs associated with detection and prevention of identity theft" survive a motion to dismiss) (citing *Resnick v. AvMed, Inc*., 693 F.3d at 1324). Equifax's failure to distinguish, or even discuss, either case is telling.

Similarly, numerous other courts have held that a claimant in a data breach case need *not* have been the actual victim of identity theft to have standing under Article III. In *Attias*, for example, the D.C. Circuit found it was plausible to infer that a hacker has both "the intent and the ability to use the data for ill," thus

---

overseas contacts might be intercepted. 568 U.S. at 404-05, 410. By contrast, numerous courts have distinguished *Clapper* and recognized that plaintiffs who have reasonably spent money to protect themselves against a substantial risk from a data breach have standing to pursue such claims. *See, e.g.*, *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628-29 (D.C. Cir. 2017), cert. denied, 138 S. Ct. 981 (2018).

creating the substantial risk of harm necessary to satisfy *Clapper*'s injury-in-fact requirement. As the court explained:

> No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken.

Attias, 865 F.3d at 629.

The Seventh Circuit has also endorsed this approach in two different cases. In *Lewert v. P.F. Chang's China Bistro, Inc*., the Seventh Circuit found that plaintiffs who faced an increased risk of future harm after a data breach from fraudulent credit card use and identity theft alleged injury sufficient to support Article III standing. 819 F.3d 963, 970, 996 (7th Cir. 2016). And, in *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 691-94 (7th Cir. 2015), another data breach case, the Seventh Circuit found that similar claims were not mere "allegations of possible future injury," but were instead the type of "certainly impending" future harm that standing requires, 794 F.3d at 692, explaining that plaintiffs "should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such injury will occur" and cautioning that "it is important not to overread *Clapper*." *Id*. at 693-94.

The Sixth Circuit has also concluded that allegations of an increased risk of future harm from identity theft or fraud, coupled with reasonably incurred mitigation costs, are sufficient at the pleading stage. *Galaria v. Nationwide Mut. Ins. Co*., 663 F. App'x 384, 385-86 (6th Cir. 2016) (unpublished). Agreeing with the logic of the Seventh Circuit in *Remijas*, the *Galaria* court noted that where a data breach targets personal information, it would be unreasonable for the plaintiffs to wait until after a thief misused their data to take steps to ensure their security because "a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes." *Id.* at 388. Therefore, although it was not "literally certain" that the plaintiffs' personal information would be misused, there was a "substantial risk" of harm that was sufficient for the plaintiffs to incur reasonable mitigation costs, thus satisfying the injury-in-fact requirement. *Id.* at 388-89.

Although the factual circumstances here are somewhat unique given the nature of the breach and the resulting claims, because the type of information that was stolen also impacted small businesses (as opposed to just individual holders of credit cards in other cases), the holdings summarized above still apply. Indeed, the sensitive nature of the data stolen and its necessity to the operations of the Small Business Plaintiffs, the direct impact of the breach on small businesses as

highlighted by Congressional committees and commentators, and the resulting need to mitigate the resulting harm all support Plaintiffs' standing in this case.

Nevertheless, Equifax attempts to characterize Plaintiffs' injuries as: "(1) the 'increased risk' of speculative future harm to their creditworthiness and continued operations; and (2) voluntary costs to mitigate the alleged risk of future harm." Mot. 13. Equifax then sets up a "straw man" of what Plaintiffs would have had to plead to prove these damages and criticizes Plaintiffs for not doing so. *Id.* at 13-14. But Equifax's arguments do not derive from any of the relevant case law summarized above, and instead promote a Rule 56 standard at the pleading stage.[2]

[2] Equifax's reliance on *Beck v. McDonald* is misplaced. In *Beck*, the Fourth Circuit distinguished the cases Plaintiffs cite *supra* because "[u]nderlying the cases are common allegations that sufficed to push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent." 848 F.3d 262, 274 (4th Cir. 2017), cert. denied sub nom. *Beck v. Shulkin*, 137 S. Ct. 2307. In *Beck*, plaintiffs sued over a stolen laptop containing their information but had "uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information." *Id.* Similarly, in *Reilly v. Ceridian Corp.*, the court found the alleged risk of identity theft was too hypothetical and speculative to establish "certainly impending" injury-in-fact because it was "not known whether the hacker read, copied, or understood" the system's information and no evidence suggested past or future misuse of employee data or that the "intrusion was intentional or malicious." 664 F.3d 38, 40, 44 (3d Cir. 2011). These are not the facts pled here.

There is no requirement to plead evidence to establish Article III standing. Because Plaintiffs adequately plead that their owners' data was stolen for nefarious purposes, that as a result they face substantial and imminent risk of harm to their business operations, and that they have spent time and incurred costs to detect and mitigate that risk such as by purchasing business credit reports and monitoring services, the injury-in-fact requirement has been satisfied. *See* Compl. ¶¶ 11-21.

C. The Alleged Injuries Are Fairly Traceable To The Breach.

Traceability requires Plaintiffs to plead "a causal connection between the injury and the conduct complained of – the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court." *Lujan*, 504 U.S. at 560 (quotations omitted). In the data breach context, this is not a particularly high bar once plaintiffs show an injury that is connected to the breach, as numerous courts, including this one, have held. *See, e.g.*, *Home Depot*, 2016 WL 2897520, at *3 ("The injuries, as pleaded, are also fairly traceable to [Defendant's] conduct, specifically the alleged failure to implement adequate data security measures."); *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 623 (4th Cir. 2018) (the "fairly traceable standard is not equivalent to a requirement of tort causation.") (internal citations omitted).

Arguments akin to the one made here by Equifax have thus been routinely rejected in data breach cases, both by this Court, *see, e.g.*, *Home Depot*, 2016 WL 2897520, at *3, and numerous appellate courts, including the Fourth, Sixth, Seventh, and Eleventh Circuits. *See Resnick*, 693 F.3d at 1324 (holding that a data breach victim's injury was fairly traceable to the defendant's negligence because "[e]ven a showing that a plaintiff's injury is *indirectly* caused by a defendant's actions" is sufficient); *Attias*, 865 F.3d at 629 (holding that although the hacker was the immediate cause of the plaintiffs' injuries, the defendant's failure to secure its customers' sensitive data was only one step removed in the causal chain, and therefore the resulting injuries were "fairly traceable" to the defendant's conduct) *Galaria*, 663 F. App'x at 390 ("[a]lthough hackers are the direct cause of Plaintiffs' injuries, the hackers were able to access Plaintiffs' data only because [defendant] allegedly failed to secure the sensitive personal information entrusted to its custody"); *Hutton*, 892 F.3d at 623-24 (holding that the alleged injuries satisfied the "fairly traceable" requirement even though the defendant denied a breach had even occurred).

As in those cases, Plaintiffs' claims here are fairly traceable to Equifax's knowing failure to secure the sensitive data that is the foundation of the modern economy. Whether, as Equifax claims, "third-party hackers" are *more* responsible

for the "Business Plaintiffs' voluntary expenditures or future harm to [their] credit or continued operations" (Mot. 19) simply has no bearing on whether Plaintiffs' injuries can *also* be traced to Equifax's failures. This is particularly true on a motion to dismiss, where the standing inquiry is much less strict than at later stages of the litigation. *Cf. Arby's*, 2018 WL 2128441, at *10 (plaintiffs adequately pleaded a causal connection to their injuries from breach to survive motion to dismiss).

Equifax's reliance on *Florida Association of Medical Equipment Dealers, Med-Health Care v. Apfel*, 194 F.3d 1227 (11th Cir. 1999), a case that does not even involve a data breach, demonstrates the weakness of its position. In *Apfel*, the court held that the plaintiff association, which sought to preliminarily enjoin a government bidding process in which its members had not yet submitted bids, lacked standing because the process was not complete and the alleged injuries thus were speculative. *Id.* at 1229. Those facts bear no resemblance to this case. Here, the data breach has already occurred, Plaintiffs have been subjected to an ongoing and imminent risk of harm, and Plaintiffs have already incurred out-of-pocket costs to mitigate the risk. Such allegations are sufficient to satisfy Article III, as the numerous data breach decisions cited by Plaintiffs above so hold.

II. SMALL BUSINESS PLAINTIFFS ADEQUATELY PLEAD A NEGLIGENCE CLAIM.

A. The Small Business Complaint Alleges A Recognized Legal Duty.

Equifax argues that it has no legal duty to protect the confidently of the information that it collects and holds. In other words, according to Equifax, it could intentionally release sensitive credit information to criminals, knowing it would harm individuals and businesses, without incurring any legal responsibility. For the reasons explained in Consumer Plaintiffs' opposition, Doc. 452 at 9-18, and briefly summarized here, the Court should not accept such an illogical proposition.

Under Georgia law, "allegations that a company knew of a foreseeable risk to its data security systems are sufficient to establish the existence of a plausible legal duty and survive a motion to dismiss." *Arby's*, 2018 WL 2128441, at *5. Put another way: "A retailer's actions and inactions, such as disabling security features and ignoring warning signs of a data breach, are sufficient to show that the retailer caused foreseeable harm to a plaintiff and therefore owed a duty in tort." *Home Depot*, 2016 WL 2897520, at *3; *see also In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1173 (D. Minn. 2014) (applying Georgia law).

The facts alleged here are even worse. Despite its critical role in the credit system and appreciation of the risk of a massive data breach, Equifax had seriously

deficient security measures, ignored repeated red flags and warnings that drastic improvements were needed, neglected to install a software patch that it knew was critical, and failed to implement basic security measures to detect and monitor unauthorized activity on its network. *See generally* Compl. ¶¶ 96-104, 136-89. Under these circumstances, Equifax owed all those who would be foreseeably impacted—including both individual consumers and their small businesses—a legal duty to use reasonable care to employ data security measures adequate to prevent a data breach from occurring. *Id.* ¶¶ 227-36 (allegations detailing duty); Consumer Opposition Brief, Doc. 452 at 9-11.

Equifax's play for immunity depends almost entirely on its strained reading of *McConnell v. Dep't of Labor*, 345 Ga. App. 669 (2018), *cert. pending*, Nos. S18C1316 and S181317 (Ga. May 31, 2018) ("*McConnell II*"). But in the original opinion, the Georgia Court of Appeals itself distinguished *Home Depot* (and by implication massive data breach cases such as this one involving similar allegations), stating:

> The district court found a duty to protect the personal information . . . in the context of allegations that the defendant failed to implement reasonable security measures . . . [despite] multiple warnings . . . and even took affirmative steps to stop its employees from fixing known security deficiencies. There are no such allegations in this case.

McConnell v. Dep't of Labor, 337 Ga. App. 457, 459 n.4 (2016) ("*McConnell I*"). Likewise, *Arby's* distinguished *McConnell*, concluding the facts in that case "are *starkly different*" from the type of data breach involved in *Home Depot* and at issue here because of the absence of "known security deficiencies" or any allegations that the action of the agency employee in 'inadvertently' emailing the spreadsheet containing the information was foreseeable." 2018 WL 2128441, at *6 (emphasis added).

Given the critical factual differences between the cases, Equifax is wrong that *McConnell* conflicts with *Home Depot* or *Arby's*. Mot. 24. There were simply no allegations in *McConnell* that the defendant should have anticipated the inadvertent disclosure of personal information by its employee. *Arby's*, 2018 WL 2128441, at *6. By comparison, here, as in *Home Depot* and *Arby's*, there are detailed, plausible allegations that the data breach was foreseeable, triggering a duty to exercise reasonable care. *Arby's*, 2018 WL 2128441, at *5; *Home Depot*, 2016 WL 2897520, at *4; *see also* Consumer Opposition Brief, Doc. 452 at 9-18.[3]

[3] Equifax again leans too heavily on *Wells Fargo Bank, N.A. v. Jenkins*, 293 Ga. 162 (2013), arguing the decision "rejected the plaintiff's argument that Georgia law imposes a duty to protect" personal information. Mot. 23. *Jenkins*, however, held only that duties imposed by the Gramm–Leach–Bliley Act, 15 U.S.C. § 6801(a), do not give rise to a cause of action for negligence under O.C.G.A. § 51-1-6. *Id.* at 165 n.4 ("the question of a legal duty under the cited provision of the

B. Equifax Owes A Tort Duty To The Small Business Plaintiffs.

Equifax next argues that even if *McConnell* does not defeat individual consumer claims, Equifax cannot owe Small Business Plaintiffs a tort duty because it did not act negligently with respect to personal information belonging to them. Mot. 24-26. But the test is not whether small businesses "owned" the information that was exfiltrated in the breach; instead it is whether they were foreseeable victims of Equifax's misconduct.[4] The complaint sets forth specific and detailed allegations sufficient to establish that, in fact, the Small Business Plaintiffs were foreseeable victims of the breach. *See, e.g.*, Compl. ¶¶ 190-94, 201, 202-05, 210, 227, 229, 231. Indeed, because Equifax sold products designed to enable small businesses to protect themselves from a data breach, that small businesses would

---

GLBA is the linchpin of the Court of Appeals holding at issue and is the precise question on certiorari"). There is a reason no court has read *Jenkins* more expansively as Equifax urges; the case simply does not decide this particular issue. *See Arby's*, 2018 WL 2128441, at *4 ("there are no Georgia appellate cases that have considered negligence claims in a large data breach involving a third party criminal hacker").

[4] Equifax cites *Queen v. Craven*, 95 Ga. App. 178, 183 (1957), for the uncontroversial proposition that "[a] negligent act is not actionable unless negligent as to the plaintiff." Mot. 25. There, a contractor completed a demolition project for a residential landlord. Upon completion and acceptance by the landlord, the contractor could not be held liable for subsequent injuries to a lessee caused by the conditions created during the demolition project. *Id.* at 183-85. At that point, under black-letter law that has no application here, the landlord was solely responsible for the dangerous condition. *Id.*

be injured by a data breach at Equifax was not only foreseeable, but actually explicitly known to Equifax.

Equifax's contention that the Small Business Plaintiffs do not allege "Equifax was negligent *as to them*," Mot. 25, both misconstrues the complaint and misses the point.[5] Equifax's legal duty arises from the fact that harm to the Small Business Plaintiffs was foreseeable, not that Equifax specifically targeted them for harm. *See Amos v. City of Butler*, 242 Ga. App. 505, 506 (2000) ("[T]he legal duty to exercise ordinary care arises from the foreseeable unreasonable risk of harm from such conduct."); *Bradley Ctr., Inc. v. Wessner*, 250 Ga. 199, 202 (1982) (duty to protect against a third person's criminal act exists when there is "reason to anticipate" the criminal act). Moreover, to be held liable for negligence, it is only necessary that Equifax could have foreseen some injury will result, not that it could have foreseen all of the potential consequences:

> With reference to foreseeability of injury, the correct rule is that in order for a party to be held liable for negligence, it is not necessary that he should have been able to anticipate the particular consequences which ensued. It is sufficient if, in ordinary prudence, he might have foreseen that some injury would result from his act or omission, and that consequences of a generally injurious nature might result.

[5] It is also a repackaging of Equifax's position on proximate causation, which as argued below presents an issue of fact for the jury and cannot be decided on a Rule 12 motion.

Corbitt v. Walgreen Co., 2015 WL 1726011 at *2 (M.D. Ga. Apr. 15, 2015) (citing *Freeman v. Wal–Mart Stores, Inc*., 281 Ga. App. 132, 136 (2006)).

Equifax's argument that the duty recognized in *Home Depot* and *Arby's* does not extend to foreseeable victims of a breach other than those whose data is stolen is unsupported by any legal citation or logic. To the contrary, in *Home Depot* and *Arby's*, the banks that benefitted from the merchants' legal duty to use reasonable care did not have their confidential data stolen; rather, the stolen data belonged to the banks' *customers*. This Court nonetheless recognized the legal duty extended to the banks because it was foreseeable that the banks would also be injured from the breach. That is the precise situation presented here. Further undercutting Equifax's argument, courts in other contexts have extended tort duties to reach foreseeable victims in much more attenuated situations. *See, e.g.*, *In re Syngenta AG MIR 162 Corn Litig.*, 131 F. Supp. 3d 1177, 1188-93, 1191 n.7 (D. Kan. 2015) (holding that a manufacturer's legal duty to avoid selling genetically modified seed that depressed the market for corn extended not only to those who sold corn in that market but also to farmers who sold other products that were foreseeably impacted, rejecting the argument that extending the duty to those farmers was too remote or would result in fraudulent or speculative claims).

Likewise, Equifax's warning that imposing a legal duty here would "expand traditional tort concepts beyond manageable bounds" and "create an almost infinite universe of potential plaintiffs," Mot. 25, rings hollow.[6] There is nothing alarming or unmanageable about allowing small businesses to recover for their foreseeable injuries, including the costs they incurred in paying Equifax for products necessary to detect and prevent the harm that Equifax's own misconduct created. Moreover, the universe of potential plaintiffs is not unlimited, but rather is comprised only of those small businesses owned by consumers whose data Equifax allowed to be stolen. That the number of such businesses may be in the millions simply reflects the scope of the breach, not the absence of definitive boundaries.

The legal authorities relied upon by Equifax, none of which involve a data breach, are unpersuasive. For example, *Rasnick v. Krishna Hospitality, Inc.*, 289 Ga. 565, 569-70 (2011), held that innkeepers do not have an affirmative duty to check on their guests to determine if they are in medical need because "the possible health problems of a guest . . . are not caused by or are unrelated to the stay at the facility." In contrast, in this case it was *Equifax*'s own conduct

[6] Contrast this case with *CSX Transp., Inc. v. Williams*, 278 Ga. 888, 891 (2005), cited by Equifax, holding that the *duty to provide a safe workplace* does not extend to *third parties outside of the workplace*. Thus, under Georgia law, companies negligently exposing their employees to asbestos at work do not have a duty to off-site third parties who later come into contact with the employees' clothing.

involving a core part of its business that foreseeably caused plaintiffs' injuries. Similarly, in *Albany Urology Clinic, P.C. v. Cleveland*, 272 Ga. 296 (2000), the court held against the plaintiff because it was unwilling to recognize a new cause of action for policy reasons not relevant here. *See* 272 Ga. at 298-303. Plaintiffs are not asking this Court to recognize a "new" tort, but rather to apply "traditional tort principles of negligence to the facts of this case." *Wessner*, 250 Ga. at 202; *see also Arby's*, 2018 WL 2128441, at *7.

The Court thus should deny the motion to dismiss the negligence claim based upon Equifax's assertion that it owned no legal duty.

C. Plaintiffs Allege The Equifax Breach Is The Proximate Cause Of Their Injuries.

Under Georgia law, the issue of proximate cause turns on foreseeability and typically is decided by a jury. *See* D. Dobbs, et al., *The Law of Torts* § 214 (2d ed. 2011) ("Courts agree that the scope of liability—commonly called proximate cause, including its subset of superseding cause problems—is to be determined on a case-by-case analysis, that it is a jury question in all but the most extreme cases, and that it turns on foreseeability in some form."); *see also, e.g., Zeagler v. Norfolk S. Ry. Co.*, 317 Ga. App. 302, 309 (2012), *aff'd* 293 Ga. 582 (2013) ("[T]he railroad might argue [at trial] that although its negligence might have been a cause-in-fact or a contributing cause-in-fact of Zeagler's injuries, such negligence was

not a proximate cause because it was too attenuated from its unfortunate consequences."); *Gen. Motors Corp. v. Davis*, 141 Ga. App. 495, 497-98 (1977) (affirming denial of summary judgment because question of whether decedent was outside of the manufacturer's "ambit of risk" was for jury).

Plaintiffs have explicitly—and plausibly—alleged that their injuries were foreseeable and proximately caused by Equifax's negligence and other misconduct. Compl. ¶¶ 11-21. Whether these allegations can be proven thus is an issue of fact for summary judgment or trial, not a matter of law to be decided on a motion to dismiss. *See, e.g.*, *Redmon v. Daniel*, 335 Ga. App. 159, 166 (2015) (proximate cause is "normally" a jury question); *Hite v. Anderson*, 284 Ga. App. 156, 158 (2007) (at motion to dismiss stage, plaintiffs must merely allege proximate cause); *In re Syngenta*, 131 F. Supp. 3d at 1193 ("[T]he foreseeability of the harm is especially pertinent to the proximate cause analysis, and plaintiffs have alleged facts to state a plausible claim that their injuries were not only foreseeable but were actually foreseen").

Equifax grudgingly acknowledges that proximate cause is almost always a jury issue, but argues this case is among the "rare" exceptions to this rule. This argument appears to be rooted in a misapprehension of the claims now before the Court. Equifax contends that the relief sought here is "duplicative" and

"derivative" of that sought by the consumer plaintiffs, but that contention is inaccurate. The Small Business Plaintiffs seek to recover *only* damages suffered by them as legal entities separate and apart from the damages sought by their individual owners—e.g., recovery of the money businesses spent from their business accounts on business credit reporting and monitoring products. To hold otherwise would wipe out the legal distinction between a corporation and its owners, a result that would be akin to barring Equifax from recovering for damage to one of its vehicles involved in a wreck because the vehicle was driven by a shareholder who suffered personal injury.

Under the circumstances, there is *no risk* of an impermissible double recovery, or the necessity of "complicated rules apportioning damages among plaintiffs removed at different levels of injury." Mot. 37 (quoting *Holmes v. Sec. Inv'r Prot. Corp.*, 503 U.S. 258, 268-70 (1992)).[7] Nor do the Small Business Plaintiffs seek "infinite liability for all wrongful acts," or implicate "an endless number of downstream plaintiffs." Mot. 36. Rather, the Small Business

[7] The theory of recovery in *Holmes* really was complicated. The SIPC sought subrogation rights of non-stock-purchasing customers who were injured "insofar as the stock manipulation first injured the broker-dealers and left them without the wherewithal to pay customers' claims. . . . The broker-dealers simply cannot pay their bills, and only [their] intervening insolvency connects the conspirators' acts to the losses suffered by the nonpurchasing customers . . . ." 503 U.S. at 271. No such "indirect injury" step is implicated by the pleading now before this Court.

Plaintiffs—a discrete number of readily identifiable entities whose welfare depends on Equifax's stewardship of their owners' credit information—are simply seeking redress for the foreseeable consequences to them from Equifax's misconduct based on the same legal claims brought by their owners.

The authorities on which Equifax relies—while accurately identifying the exceptionally rare cases where the Georgia courts determine proximate cause without a jury—do not support dismissal of the small business claims. Each case turns on complicated questions of foreseeability or a chain of attenuated events involving claims for personal injury or business interruption losses.[8] These cases, which resurrect hornbook legal analysis of unforeseeable consequences that

[8] *See, e.g.*, *Byrd v. English*, 117 Ga. 191 (1903) (business interruption from severing of power line through which plaintiff had contractual right to receive power from electric company); *Union Camp Corp. v. S. Bulk Indus., Inc.*, 193 Ga. App. 90 (1989), *aff'd*, 259 Ga. 828 (1990) (negligent damage to water supply line while constructing a holding pond interrupted water supply to defendant); *Willis v. Georgia N. Ry. Co.*, 169 Ga. App. 743 (1984) (railroad not liable to workers for loss of wages due to railroad's negligence in allowing railcars to roll down spur track into plant requiring shutdown of plant for repairs); *Remax The Mountain Co. v. Tabsum, Inc.*, 280 Ga. App. 425 (2006) (no claim for businesses alleging that detour necessitated by defendants' negligent dumping of groundwater caused them to lose profits); *Dowdell v. Wilhelm*, 305 Ga. App. 102, 105-06 (2010) (wrongful death action against sheriff's deputies alleging deputies' negligence permitted prisoner to escape from confinement and kill plaintiff widow's husband in home); *W. Stone & Metal Corp. v. Jones*, 180 Ga. App. 79 (1986) (post-trial ruling where shop owner negligently set off the shop's silent alarm; as police responded to the call, a pedestrian was startled by emergency vehicles, fell, and injured her hip).

underlie decisions such as *Palsgraf v. Long Island R. Co.*, 248 N.Y. 339 (1928) and *Petition of Kinsman Transit Co.*, 338 F.2d 708 (2d Cir. 1964), are readily distinguishable from a case such as this one that involves objectively foreseeable victims and injuries. Indeed, Equifax not only foresaw the victims and injuries, but even before (and after) the breach offered to sell the victims products to detect and prevent the specific harm that, incredibly, Equifax now alleges is too remote to support legal liability as a matter of law.[9]

Finally, Equifax cannot avoid liability for its own conduct at this stage by blaming the hackers and asserting the breach was unforeseeable because it resulted from criminal activity. Mot. 37-38. Equifax's assertion is not grounds for dismissal—it raises an issue, if at all, for the jury. *See Sturbridge Partners, Ltd. v. Walker*, 267 Ga. 785, 786 (1997) (foreseeability is for jury). An intervening criminal act does *not* insulate a defendant from liability as a matter of law where, as here, "it is alleged that the defendant had reason to anticipate the criminal act." *Atlantic Coast Line R. Co. v. Godard*, 211 Ga. 373, 377 (1955); *Wessner*, 250 Ga. at 202 (same); *Landis v. Rockdale County*, 206 Ga. App. 876, 881 (1992) (same).

[9] Another of Equifax's proffered analogous cases actually involved a failure of proof (causation-in-fact) to support the plaintiff's theory of liability. *Walker v. CSX Transp. Inc.*, 650 F.3d 1392, 1398-1402 (11th Cir. 2011) (no evidence linking a railroad worker's injury to a discoverable and curable defect in particular railroad machinery).

The Court should therefore reject Equifax's reliance on *Andrews v. Kinsel*, 114 Ga. 390 (1901), which did not involve any allegations that the criminal act was foreseeable, and instead apply longstanding black-letter law that supports Plaintiffs' position. *See, e.g.*, *Arby's*, 2018 WL 2128441, at *3-4 (rejecting the argument that hackers are an unforeseeable intervening cause).

D. The Economic Loss Rule Does Not Bar Small Business Plaintiffs' Tort Claims.

As it did in its motion to dismiss the consumer claims, Equifax ignores the fact that this Court has twice rejected the application of the economic loss rule to data breach cases, holding that the rule does not apply when there is an "independent duty of care." *Arby's*, 2018 WL 2128441, at *12-14; *Home Depot*, 2016 WL 2897520, at *3-4. The duty to safeguard sensitive credit information in the face of a foreseeable security threat is a duty independent of any contract. *See id.* at *4; *Arby's*, 2018 WL 2128441, at *5. Equifax's authorities are inapposite because they did not involve an independent duty. *See, e.g.*, *City of Atlanta v. Benator*, 310 Ga. App. 597, 606 (2011) ("Based upon the particular facts and circumstances of this case, we decline to find the existence of a duty independent of contract . . . ."). Plaintiffs' claims thus are not barred by the economic loss rule.

E. Small Business Plaintiffs Allege Legally Cognizable Harms.

Similar to its standing arguments, Equifax asserts that Plaintiffs have not alleged "any legally cognizable harms they suffered as a result of the breach." Mot. 28. But as recognized by the Seventh Circuit, "[t]o say that the plaintiffs have standing is to say that they have alleged injury in fact, and if they have suffered an injury then damages are available." *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018). In other words, the injuries alleged here "can justify money damages, just as they support standing." *Id*.

In this case, as noted above, Plaintiffs have alleged two types of harms that are both explicitly acknowledged by Equifax: (1) the substantially certain risk that Plaintiffs face to business operations from the impact to their owners' creditworthiness from the breach; and (2) the mitigation costs and devotion of time and resources Small Business Plaintiffs incurred in responding to the breach. Mot. 29. These allegations support cognizable harms as the result of the data breach.

Equifax repeatedly refers to Plaintiffs' business harms as an "increased *risk* of highly speculative future harms." Mot. 30 (emphasis in original). This mischaracterizes Plaintiffs' claims. While not every breach poses a substantial risk to small businesses, this breach does so because the hackers stole highly sensitive data from one of the three major credit reporting agencies pertaining to the owners

of those businesses, including credit worthiness data that impacts the businesses' own ability to obtain and maintain credit. Given the direct and substantially certain risk to small business owners' credit from this breach, the small business harms as alleged in the complaint are cognizable.

Moreover, Equifax wrongly asserts that a risk of future harm is never legally valid. As the Supreme Court has recognized, future harm is a cognizable injury when it is either "certainly impending" *or* the risk is "substantial." *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014). Plaintiffs allege both an impending and substantial risk of future harm, which only makes sense since the compromised information was stolen by criminals in order to misuse it. *See, e.g.*, *Attias*, 865 F.3d at 629 ("[A] substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken"); *Galaria*, 663 F. App'x at 387-89 ("There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals").

Importantly, as Equifax concedes, the Small Business Plaintiffs also plead that they have incurred costs "in the form of a business credit report and devotion of resources to monitoring [their] financial accounts" in response to the "substantial risk of harm from the breach." Compl. ¶¶ 12-21. These costs are

cognizable harm. *See, e.g.*, *Home Depot*, 2016 WL 2897520, at *3; *Arby's*, 2018 WL 2128441, at *11 (monetary losses related to fraudulent charges, theft of personal financial information, and costs associated with detection and prevention of identity theft sufficient); *Hutton*, 892 F.3d at 622-23, n.9 (4th Cir. 2018) (costs of taking mitigating measures, drop in credit score, and time lost dealing with repercussions of data breach constitute injuries); *see also Attias*, 865 F.3d at 627; *Resnick*, 693 F.3d at 1323.

Equifax's reliance on *Collins v. Athens Orthopedic Clinic* (Mot. 30-31) is unavailing. While the court in *Collins* upheld dismissal of a data breach case where the plaintiffs alleged potential future costs associated with lifetime credit monitoring or credit freezes, plaintiffs there (unlike those here) did not allege any *current* out of pocket losses tied to the breach. --- Ga. App. ---, 815 S.E.2d 639 (2018). Moreover, the opinion, which is not binding precedent because it was not unanimous (Ga. Ct. App. R. 33.2(a)(1)), is inapplicable. Because the *Collins* plaintiffs alleged *only* an "increased risk of harm," the court found that future costs for "credit monitoring and other precautionary measures" were not recoverable, and limited the decision to the "facts before us." *Id*. at 645. In so doing, the court distinguished *Arby's* and *Resnick* because in those cases the plaintiffs pled "costs associated with actual data theft" and actual "financial injury" as a result of the

breaches. *Id.* at 644. Plaintiffs here plead out-of-pocket costs and devotion of time and resources to mitigate harm.

Finally, to the extent Equifax questions whether Plaintiffs' mitigation expenses were necessary or recoverable, those are jury issues. *See P.F. Chang's*, 819 F.3d at 969 ("[A]ll class members should have the chance to show that they spent time and resources tracking down the possible fraud, changing automatic charges, and replacing cards as a prophylactic measure."); *Arby's*, 2018 WL 2128441, at *11 n.12 ("[I]n the Court's view, a consumer's time and effort to remediate the effects of a breach is not an abstract notion of actual damage and one that is susceptible to proof and valuation by a jury.").

III. SMALL BUSINESS PLAINTIFFS ADEQUATELY ALLEGE NEGLIGENCE PER SE.

Equifax's arguments for dismissal of Small Business Plaintiffs' claim for negligence per se are the same as those made in support of its motion to dismiss the main consumer complaint and are without merit for the same reasons. Under Georgia law, violation of a statute or regulation that serves as a standard of conduct constitutes negligence per se. *See, e.g., Pulte Home v. Simerly*, 322 Ga. App. 699, 705-06 (2013). A plaintiff must show that he or she is within the class of persons the statute was intended to protect and the statute was intended to protect against

the harm suffered. *See, e.g., Amick v. BM & KM, Inc.*, 275 F. Supp. 2d 1378, 1382 (N.D. Ga. 2003).

Small Business Plaintiffs assert a negligence per se claim premised on Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits unfair or deceptive trade practices.[10] The failure to maintain reasonable data security measures to safeguard confidential consumer information is an unfair practice prohibited by the Act. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015).[11] Plaintiffs here allege Equifax violated Section 5 by not having reasonable data security, they are within the class the section was intended to protect, and the section was meant to protect against the harm that occurred. Compl. ¶¶ 243-47.

---

[10] Plaintiffs also state negligence per se claims predicated on various state statutes modeled after Section 5, such as the Georgia Fair Business Practices Act. Compl. ¶¶ 243-46. The same rationale that supports Plaintiffs' negligence per se claim under Section 5 also supports these claims predicated on analogous state statutes.

[11] For the entire decade leading up to the Equifax breach, the FTC published the "Guide for Business" on "Protecting Personal Information," which provided a catalog of reasonable data security practices including, for example, that companies "implement policies for installing vendor-approved patches to correct problems." Federal Trade Commission, Protecting Personal Information, A Guide for Business, p.10, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Sept. 12, 2018). In that same time period, the FTC obtained more than 50 data security settlements through enforcement of Section 5 of the FTC Act. *See* Commission Statement Marking the FTC's 50th Data Security Settlement, Jan. 31, 2014, https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf (last visited Sept. 12, 2018).

Such allegations properly state a claim for negligence per se under Section 5, as at least three courts have held in other data breach cases. *See, e.g.*, *Home Depot*, 2016 WL 2897520, at *4; *Arby's*, 2018 WL 2128441, at *8-9; *First Choice Fed. Credit Union v. Wendy's Co.*, 2017 WL 9487086, at *4 (W.D. Pa. Feb. 13, 2017), *report and recommendation adopted*, 2017 WL 1190500 (W.D. Pa. Mar. 31, 2017). None of Equifax's arguments to the contrary should prevail.

First, Equifax argues Section 5 is "not specific enough" to create a statutory duty. Mot. 41. But this argument was summarily rejected in *Arby's*, *Home Depot*, and *Wendy's*, *see Arby's*, 2018 WL 2128441, at *8, and Equifax does not even attempt to explain why those decisions are wrong. Further, "two circuit courts have expressly held that 'unfair' or 'deceptive' trade practices under Section 5 of the FTCA fairly encompass the failure to provide adequate data security measures to protect consumer financial data from threat of hacking." *Id.* (summarizing *Wyndham*, 799 F.3d at 247 and *In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 498 (1st Cir. 2009)).

In persisting to argue that only a specific duty, rather than a generalized standard of conduct such as the requirement to maintain reasonable data security, can support a claim for negligence per se, Equifax also ignores contrary Georgia law. As the Georgia Supreme Court has held, "Where a statute provides a general

rule of conduct, *although only amounting to a requirement to exercise ordinary care*, the violation thereof is negligence as a matter of law, or negligence per se." *Teague v. Keith*, 214 Ga. 853, 853-54 (1959) (emphasis added) (noting that negligence per se claim can be based on statutes prohibiting a driver from driving at a "speed greater than is reasonable").

Similarly, Equifax's citation to *Brock v. Avery Co.*, 99 Ga. App. 881, 886 (1959) is unavailing. Mot. 41. Indeed, if the Court of Appeals' decision in that case had the meaning Equifax attributes to it, *Brock* would be inconsistent with (and thus effectively overruled by) the Georgia Supreme Court's decision in *Teague* cited above. Regardless, while the court in *Brock* did find that a rule of the road regarding obstruction of traffic was "too indefinite for enforcement," the court also noted that the same rule of the road "does furnish a rule of civil conduct under the circumstances of each case, and the jury may find negligence in fact as a result of its violation." 99 Ga. App. at 886. This language parrots modern language regarding negligence per se. *Compare id. with Pulte Home*, 322 Ga. App. at 705 ("It is well-settled that Georgia law allows the adoption of a statute or regulation as *a standard of conduct* so that its violation becomes negligence per se.") (emphasis added). Thus, *Brock* does not support Equifax's argument; even if Section 5 was an

"indefinite" rule, it can still serve as the source of standards of conduct sustaining Plaintiffs' claims here.

Second, Equifax misreads the Eleventh Circuit's decision in *LabMD, Inc. v. F.T.C.*, 894 F.3d 1221 (11th Cir. 2018). According to Equifax, *LabMD* holds that a practice must violate clear policies established under the common law to be unfair under Section 5 and, because the common law imposes no duty to maintain reasonable data security, Equifax could not have violated Section 5. However, the Eleventh Circuit did not hold the common law imposes no such duty, but in fact assumed that a common law duty exists, citing the Restatement (Second) of Torts. *See id.* at 1231. The court vacated the FTC's order at issue because the order was too vague to be enforced—an issue not presented here—not because inadequate data security cannot be regulated under Section 5.[12] *See id*. at 1236-37.

[12] Equifax's argument that inadequate data security is not an unfair practice under Section 5 rests on the assertion that Georgia common law imposes no duty on Equifax to safeguard confidential information, which is incorrect for the reasons discussed previously. Regardless, Section 5 is a federal statute and, as such, applies uniformly throughout the nation and preempts contrary state law. Accordingly, the *LabMD* court did not examine the law in the defendant's home state, but rather the common law generally as expressed in the Restatement. 894 F.3d at 1231. To adopt Equifax's rationale would mean that Section 5 must be construed differently depending on the state in which the conduct at issue occurred, a novel proposition for which Equifax provides no authority.

Third, Equifax conflates implied rights of action with negligence per se. Mot. 42-43. Georgia law is clear that negligence per se claims are cognizable even if the predicate statute contains no private right of action. *See Pulte Home*, 322 Ga. App. at 707; *see generally* O.C.G.A. § 51-1-6. This includes negligence per se claims grounded upon violations of the FTC Act. *See Home Depot*, 2016 WL 2897520, at *4 & n.66 (citing *Bans Pasta, LLC v. Mirko Franchising, LLC*, 2014 WL 637762, at *13-14 (W.D. Va. Feb. 12, 2014) (applying Georgia law) and *Legacy Acad., Inc. v. Mamilove, LLC*, 328 Ga. App. 775, 790 (2014), *aff'd in part and rev'd in part on other grounds*, 297 Ga. 15 (2015)).[13] Unsurprisingly, Equifax provides no authority for its insinuation that negligence per se claims are no longer viable in any context.

Finally, Equifax argues Small Business Plaintiffs have no valid claim under Section 5 because the FTC has not adopted a formal regulation regarding data security, but only issued directives through publications and enforcement orders. But there is no requirement that the FTC issue formal regulations to designate a

[13] As the citation indicates, the *Mamilove* litigation had a tangled appellate history, and the Court of Appeals opinion had three judges concurring and dissenting in part. It is noteworthy that as to the division of the Court of Appeals opinion discussing negligence per se and the FTC Act, all seven judges joined. On review, the Georgia Supreme Court did not disturb that section of the opinion, although it did reverse other sections. Thus, whether the FTC Act can sustain a negligence per se claim is not controversial.

practice as unfair. *See LabMD*, 894 F.3d at 1232 ("Because Congress thought impossible the task of legislating a comprehensive list of unfair acts or practices, it authorized the Commission to establish unfair acts or practices through case-by-case litigation. . . . [O]nce an act or practice is adjudged to be unfair, the act or practice becomes in effect—like an FTC-promulgated rule—an addendum to Section 5(a)."). Moreover, Georgia law does not require that a governmental directive be expressed in a statute or regulation to be enforceable. *See Jenkins*, 293 Ga. at 165 (recognizing that negligence per se can be based on a common law principle or any "regulation, *directive*, or *standard*" authorized by law) (emphasis added). Small Business Plaintiffs' claim for negligence per se thus cannot be dismissed.

IV. SMALL BUSINESS PLAINTIFFS STATE A CLAIM UNDER THE GEORGIA FAIR BUSINESS PRACTICES ACT.

The Georgia Fair Business Practices Act ("GFBPA") provides a remedy to persons harmed by "unfair or deceptive practices." O.C.G.A. §§ 10-1-391(a); 399(a). As a remedial statute, it "is to be liberally construed and applied to promote its underlying purposes and policies, which are to protect consumers." *Georgia Receivables, Inc. v. Welch*, 242 Ga. App. 146, 146 (2000). "Except in plain and indisputable cases, the question of whether a particular act or omission, or a series thereof, constitutes unfair or deceptive acts or practices within the meaning of

O.C.G.A. § 10-1-393 generally is for jury resolution." *Regency Nissan, Inc. v. Taylor*, 194 Ga. App. 645, 648 (1990). The Small Business Plaintiffs have plausibly stated all elements of a GFBPA claim.[14] *See* Compl. ¶¶ 248-260. Equifax's arguments with respect to the GFBPA claim are again a rehash of the motion to dismiss the main consumer complaint. The Court should deny the motion for several reasons:

First, Equifax again marginalizes the GFBPA ruling in *Arby's*, which was decided after *McConnell* and held that data breach victims have a claim under the GFBPA. *See In re Arby's Rest. Grp. Inc. Litig.*, 317 F. Supp. 3d 1222, 1228 (N.D. Ga. June 28, 2018) (second Rule 12(b)(6) order denying motion to dismiss amended GFBPA claim). Equifax also misconstrues *McConnell*, which says only that the Georgia statutory prohibition on displaying Social Security numbers (O.C.G.A. § 10-1-393.8) and the data breach notification statute (O.C.G.A. § 10-1-910) are not the basis of a general tort duty. *McConnell II*, 345 Ga. App. at 676-79. Unlike Plaintiffs, the *McConnell* plaintiffs did not assert a GFBPA claim. *See* Br.

[14] Equifax argues for a heightened pleading standard under the GFBPA, arguing Plaintiffs "have not even pleaded that they, or their individual owners, read and relied on any representations made by Equifax." Mot. 46 n.10. But that is more than is required, as "logic dictates that plaintiffs alleging misconduct by omission or passive conduct . . . will be less able to specify the details of the wrongdoing . . . ." *In re Arby's Rest. Grp. Inc. Litig.*, 317 F. Supp. 3d 1222, 1224, 1227 (N.D. Ga. June 28, 2018) (rejecting heightened pleading standard under GFBPA).

of Appellant, *McConnell v. Dep't of Labor*, 2017 WL 5194734, at *24. Thus, *McConnell* did not consider the issue presented here. Nor did it discuss the impact of judicial and agency interpretations of Section 5, which are incorporated into the GFBPA by the terms of the statute, O.C.G.A. § 10-1-391(b).

Second, Equifax argues that Plaintiffs could not have relied on its misrepresentations and omissions because Equifax collects data without their consent and because neither Small Business Plaintiffs nor their owners could opt out of Equifax's data collection practices. Mot. 45. This argument ignores Plaintiffs' allegations that Equifax has a special role in the modern economy in which CRAs are authorized to gather Plaintiffs' owners' confidential information and, in highly regulated circumstances, disseminate that information for the common good.[15] *See, e.g.*, Compl. ¶¶ 1, 30-54. And Equifax's actions have a direct impact on small businesses, which Equifax itself has acknowledged by selling them business-credit products to protect themselves. *See id*. ¶¶ 5, 190-211.

[15] Equifax itself seemingly acknowledges this special role, explaining, "We have built our reputation on our commitment to deliver reliable information to our customers . . . and to protect the privacy and confidentiality of personal information about consumers." Compl. ¶ 60. And the company did so again in apologizing for the breach, stating: "Equifax was entrusted with Americans' private data and we let them down." *Id.* ¶ 187.

The reality is that all of the actors in the modern economy—including small businesses, consumers, data furnishers, and regulators—relied to their detriment on Equifax's actions. By misrepresenting the truth regarding its commitment to data security and failing to disclose that its existing security measures were nearly non-existent, Equifax deprived the marketplace, including these Plaintiffs, of critical information needed to make informed decisions. Compl. ¶ 256; *see also id.* ¶ 237 (describing ways that Plaintiffs could have mitigated or ameliorated damages from Equifax's misconduct had they known the breach). Had the truth been known, Small Business Plaintiffs and the other actors could have taken protective action, such as refusing to do business with Equifax and those who furnished data to Equifax, or otherwise adjusting their behavior. *Id.* ¶ 256. These allegations of reliance thus are sufficient at the pleading stage.

Regardless, Plaintiffs need not plead reliance to state a GFBPA claim based on omissions as opposed to misrepresentations, as Plaintiffs have done. Reliance is not an express statutory element. *See* O.C.G.A. §§ 10-1-393 & 10-1-399(a); *Johnson v. GAPVT Motors, Inc.*, 292 Ga. App. 79, 84 (2008) (elements are "violation of the Act, causation, and injury"). While Georgia courts, writing in broad strokes, have characterized the GFBPA as requiring reliance, those cases turn on affirmative deception or misrepresentation theories, not omissions. *See*,

e.g., *Tiismann v. Linda Martin Homes Corp.*, 281 Ga. 137, 141 (2006) ("[H]e cannot show that he placed any reliance on LMH's allegedly deceptive *misrepresentation*") (emphasis added); *Zeeman v. Black*, 156 Ga. App. 82, 87 (1980) ("[A] claimant who alleges the FBPA was violated *as the result of a misrepresentation* must demonstrate . . . the reliance upon the alleged misrepresentation.") (emphasis added). The holdings in those cases make sense. Without proof of reliance, a plaintiff cannot establish that the misrepresentation made any difference and thus cannot prove causation.

In contrast, under an omission theory, to prove that the omission mattered—and thus establish causation—a plaintiff would be hard-pressed to show reliance upon or even awareness of the fact that the defendant failed to disclose the truth. The critical question is whether the plaintiff would have acted differently had the truth been disclosed. *See Skeen v. BMW of N. Am., LLC*, 2014 WL 283628, at *11 (D.N.J. Jan. 24, 2014) (denying dismissal of part of GFBPA claim based on fraudulent omissions); *accord In re Anthem*, 2016 WL 3029783, at *35 (N.D. Cal. May 27, 2016) ("[R]eliance can be proved in a fraudulent omission case by establishing that had the omitted information been disclosed, the plaintiff would have been aware of it and behaved differently."); *In re Adobe Sys. Privacy Litig.*, 66 F. Supp. 3d 1197, 1231 (N.D. Cal. 2014) (same). Plaintiffs allege just

that—namely, had it been known that Equifax was unwilling or unable to secure confidential consumer data, they and other economic actors would have made different decisions, required Equifax to clean up its act, or forced Equifax out of business.

Similarly, there is no logical reason to require reliance when, as here, Plaintiffs allege Equifax committed "unfair acts and practices" separate and apart from acts of deception. Compl. ¶¶ 253-254, 258; *see In re Arby's*, 317 F. Supp. 3d at 1226-27 (recognizing that under GFPBA a plaintiff "may proceed under an 'unfairness' theory," distinct from a "deception" theory). An "unfair" act is not necessarily deceptive. This is reflected in the text of O.C.G.A. §10-1-393. First, it declares that "[u]nfair *or* deceptive acts or practices" are unlawful. O.C.G.A. §10-1-393. Then, in providing a non-exhaustive list of such unfair or deceptive practices, the statute lists some acts as more unfair than deceptive. *Id.* To require reliance in such cases would deprive the victim of any remedy and thus gut GFBPA's unfairness prong. For that reason, courts in other states have construed similar statutes as not requiring reliance in unfair practice cases. *See Yue v. Conseco Life Ins. Co.*, 282 F.R.D. 469, 476-77 (C.D. Cal. 2012) ("[R]elief under the [California UCL] is available without individualized proof of deception, reliance and injury" where plaintiff pursues "unlawful" or "unfair" prongs); "Right

to Privacy Action Under State Consumer Protection Act – Preconditions to Action," 117 A.L.R.5th 155, § 10[b]. The same logic applies here.

Third, Equifax asserts that no Small Business Plaintiff alleged any cognizable injury from their violations of the GFBPA, but that is plainly contradicted by the allegations in the Complaint. *See, e.g.*, Compl. ¶¶ 11-21, 194, 247.

Finally, Equifax asserts that class actions are not permitted under the GFBPA, Mot. 47 n.11, but in the same breath acknowledges that Rule 23 overrides state statutory restrictions on representative actions. *Lisk v. Lumber One Wood Preserving, LLC*, 792 F.3d 1331, 1334-35 (11th Cir. 2015) (applying *Shady Grove Ortho. Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393 (2010)). Equifax's assertion thus fails. *See Arby's*, 2018 WL 2128441, at *19.

V. SMALL BUSINESS PLAINTIFFS ABANDON THEIR CLAIM OF UNJUST ENRICHMENT.

Because, unlike the other claims at issue here, the unjust enrichment claim in the Small Business Complaint is similar to the unjust enrichment claim pleaded by the consumer plaintiffs, it might be argued that those claims could result in an "impermissible double discovery," an issue identified repeatedly in Equifax's motion. Thus, to streamline the case as a whole consistent with Rule 1, Small Business Plaintiffs abandon their claim for unjust enrichment.

VI. SMALL BUSINESS PLAINTIFFS SUFFICIENTLY INVOKE O.C.G.A. § 13-6-11.

Under O.C.G.A. § 13-6-11, a plaintiff is entitled to recover fees and expenses as part of damages if the defendant has acted in bad faith, been stubbornly litigious, or caused unnecessary trouble or expense. This standard is met where the defendant through egregious misconduct has created a foreseeable risk of injury to others. *See, e.g.*, *Lewis v. D. Hays Trucking, Inc.*, 701 F. Supp. 2d 1300, 1312-13 (N.D. Ga. 2010) (driving a truck after driver was told he failed a DOT physical); *Ford Motor Co. v. Stubblefield*, 171 Ga. App. 331, 342 (1984) (selling an automobile despite knowledge it was defective). It is not necessary that the defendant's conduct rise to the level of an intentional tort. *Windermere, Ltd. v. Bettes*, 211 Ga. App. 177, 179 (1993). Plaintiffs plausibly allege that Equifax's conduct leading up to the breach was egregious and that both the breach and injury that resulted were foreseeable, precluding resolution at this stage of whether Plaintiffs are entitled to recovery under O.C.G.A. § 13-6-11.

CONCLUSION

For the reasons stated herein, and based on the detailed allegations in the Complaint, the Court should deny Equifax's motion to dismiss the claims of the Small Business Plaintiffs.

Dated: September 13, 2018

Respectfully submitted,

/s/ Amy E. Keller
Amy E. Keller
Adam J. Levitt
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602
Tel. 312.214.7900
akeller@dlcfirm.com
alevitt@dlcfirm.com

/s/ Norman E. Siegel
Norman E. Siegel
Barrett J. Vahle
J. Austin Moore
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel. 816.714.7100
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com

Consumer Plaintiffs' Co-Lead Counsel

/s/ Kenneth S. Canfield
Kenneth S. Canfield
Georgia Bar No. 107744
DOFFERMYRE SHIELDS CANFIELD & KNOWLES, LLC
1355 Peachtree Street, N.E.
Suite 1900
Atlanta, Georgia 30309
Tel. 404.881.8900
kcanfield@dsckd.com

Roy E. Barnes
John R. Bevis
J. Cameron Tribble
BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, Georgia 30060
Tel. 770.227.6375
roy@barneslawgroup.com
bevis@barneslawgroup.com
ctribble@barneslawgroup.com

David J. Worley
EVANGELISTA WORLEY LLC
8100A Roswell Road Suite 100
Atlanta, Georgia 30350
Tel. 404.205.8400
david@ewlawllc.com

Consumer Plaintiffs' Co-Liaison Counsel

Rodney K. Strong
GRIFFIN & STRONG P.C.
235 Peachtree Street NE, Suite 400
Atlanta, Georgia 30303
Tel. 404.584.9777
rodney@gspclaw.com

Consumer Plaintiffs' State Court Coordinating Counsel

Andrew N. Friedman
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue, NW
Suite 500
Washington, D.C. 20005
Tel. 202.408.4600
afriedman@cohenmilstein.com

Eric H. Gibbs
David M. Berger
GIRARD GIBBS LLP
505 14th Street
Suite 1110
Oakland, California 94612
Tel. 510.350.9700
ehg@classlawgroup.com

James Pizzirusso
HAUSFELD LLP
1700 K Street NW Suite 650
Washington, D.C. 20006
Tel. 202.540.7200
jpizzirusso@hausfeld.com

Ariana J. Tadler
MILBERG TADLER PHILLIPS GROSSMAN LLP
One Penn Plaza
19th Floor
New York, New York 10119
Tel. 212.594.5300
atadler@milberg.com

John A. Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel. 813.223.5505
jyanchunis@forthepeople.com

William H. Murphy III
MURPHY, FALCON & MURPHY
1 South Street, 23rd Floor
Baltimore, Maryland 21224
Tel. 410.539.6500
hassan.murphy@murphyfalcon.com

Jason R. Doss
THE DOSS FIRM, LLC
36 Trammell Street, Suite 101
Marietta, Georgia 30064
Tel. 770.578.1314
jasondoss@dossfirm.com

Consumer Plaintiffs' Steering Committee

CERTIFICATE OF COMPLIANCE

I hereby certify pursuant to L.R. 7.1D that the foregoing complies with the font and point selections permitted by L.R. 5.1C. This brief was prepared on a computer using the Times New Roman font (14 point).

/s/ Norman E. Siegel

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing was filed with this Court via its CM/ECF service, which will send notification of such filing to all counsel of record this 13th day of September, 2018.

/s/ Norman E. Siegel